REMARKS

Rejection of claims 1-16 based on 35 USC § 103(a)

Claims1-8 and 10-15 were rejected under 35 USC § 103(a) as being unpatentable over USP 6,701,437 to Hoke et al. ("Hoke") in view of USP 7,068,790 to Elliott ("Elliott") and further in view of Federal Information Processing Standards Publication (FIPS) 140-2 ("FIPS"). Claims 9, 10 and 16 were rejected under essentially the same basis. The obviousness rejections set forth in the Second office action are essentially the same as set forth in the First office action, but with an express reference to FIPS standards.

The law regarding obviousness rejections

A rejection based on obviousness requires that the Examiner make out a *prima facie* case, "without which the applicant is entitled to grant of the patent." (see, e g.., *In re Oeticker*, 24 USPQ 2d 1442, 1444 (Fed. Cir. 1992)).

As stated in MPEP § 706.02 (j), a *prima facie* case for obviousness requires:

(1) some suggestion or motivation to modify the references;

(2) a reasonable expectation of success; and

(3) the references when combined must teach or suggest all the claimed limitations.

Making out a *prima facie* case involves conducting a factual inquiry based on the so-called *Graham Factors* recently re-enunciated by the Supreme Court in *KSR International Co. v. Teleflex, Inc.*, 82 USPQ2d 1385, 1391 (2007), and as discussed in MPEP § 2141.

The *Graham Factors* are:

a) ascertaining the scope and content of the prior art;

b) ascertaining the differences between the claimed invention and the prior

art; and

c) resolving the level of ordinary skill in the pertinent art.

In determining the differences between the prior art and the claims, the question under 35 USC §103 is not whether the differences themselves would have been obvious, but whether ***the claimed invention as a whole*** would have been obvious. *Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 1537 (MPEP 2141.02(I) (emphasis added).

Obviousness rejection

In the Second office action on page 7, item 21, the Examiner states her disagreement with the Applicant's position that "Hoke nor Elliot [sic: Elliott] disclose a VPN type communication system that uses FIPS and classical encryption." Applicant does not understand the basis for this statement because the Applicant has not made this assertion. Thus, there appears to be some confusion as to the precise nature of Applicant's arguments that traverse the obviousness rejection.

Applicant therefore reformulates and clarifies its arguments here and respectfully requests the Examiner closely consider these arguments in assessing the patentability of claims 1-16.

Hoke

Hoke discloses a computer system for processing communications in a virtual private network (VPN). FIG. 1 of Applicant's Application, and page 3, lines 3-16 therein, essentially describes the teaching of Hoke as it relates to the invention claimed in the Application, namely a VPN system that uses classical encryption and that is FIPS compliant with respect to classical encryption. However, Applicant respectfully submits that with respect to Hoke, the following two points are indisputable:

1. **Hoke does not disclose or teach, suggest, or provide any motivation for using QKD techniques in combination with its VPN system.**

2. **Hoke does not disclose, teach or suggest the use of FIPS in connection with sending QKD-encrypted signals over the VPN.**

Elliott

Elliott discloses systems and methods for setting up a path in a QKD network. The invention of Elliot involves establishing paths through an optical network to a data distribution endpoint. The paths to the data distribution endpoint can be changed via optical switches if eavesdropping is discovered in the path originally used. In Elliot, the quantum keys are used to encrypt the data directly, as is normally done in QKD communication systems.

Applicant therefore submits that the following points regarding Elliott are indisputable:

1. **There is no discussion of VPN-type communication in Elliott.**
2. **Elliott does not disclose, teach or suggest anything even remotely related to FIPS standards.**
3. **The QKD-based network system disclosed by Elliot would need to go through the FIPS certification process to be FIPS compliant.**

Claims must be read as a whole and the Graham Factors properly applied

Applicant respectfully submits that the Examiner is not reading and understanding Applicant's claim as a whole, and is selectively reading both Hoke and Elliott out of context and impermissibly selecting specific items in these references to piece together Assignee's claimed invention.

An obvious analysis under the *Graham Factors* require that Applicant's claimed invention be read ***as a whole***. This includes understanding the invention in its entirety and the purpose of the invention as it is claimed. Further, the *Graham Factors* require that the ***scope*** and ***content*** of the prior art be properly construed.

Keeping these critical points in mind, a person of ordinary skill in the art would not think to use Elliott, which relates to the switching of optical paths in an optical network that uses direct QKD encryption, as the basis for achieving FIPS-compliant QKD encryption. And Hoke simply does not address the issue of FIPS compliance in the context of QKD encryption. There is simply no nexus between the inventions of Hoke and Elliot that would lead one skilled in the art to try to achieve FIPS compliance of a QKD system via a classical encryption device.

Assignee's claimed invention is directed to a VPN-type communication system that uses both quantum (i.e., QKD-based) encryption that is not FIPS-certified in combination with classical encryption that is FIPS certified. This immediately makes the system ***as a whole*** FIPS-certified while also providing ***QKD-based encryption***.

In connection with reading and understanding Applicant's claimed invention as a whole, an important point to understand is that ***the classical encryption step does not add any significant additional security to the system***. The high degree of security provided is due to the QKD system integrated therewith. Intertwining the classical and QKD encryption is a non-obvious way of "hiding" the QKD aspect of the encryption beneath the FIPS-certified classical encryption in a manner that maintains the FIPS certification while at the same time allows for the "certified" use of QKD encryption.

Assignee respectfully submits that it is ***counterintuitive*** to include both ***classical*** encryption and ***quantum encryption*** in a ***single*** communication system to achieve a ***FIPS-certified*** system having quantum security. In fact, Assignee's claimed system represents (to the best of Assignee's knowledge) the ***first*** FIPS-certified QKD-based encryption system.

Obtaining FIPS certification

Reading Applicant's claimed invention as a whole includes understanding that the usual approach to obtaining FIPS certification for a QKD system is to go through a ***rigorous, multi-year process*** of showing compliance with all of the different FIPS requirements. Because QKD systems are based on a relatively new technology, it is

generally understood that obtaining FIPS certification will take ***many years***. Assignee's claimed invention provides ***immediate*** FIPS-certified quantum encryption.

Level of ordinary skill in the pertinent art must be based in reality

The Examiner's position that it would be "obvious" to combine Hoke and Elliott to achieve Applicant's claimed invention is completely undermined by the reality of what is actually happening in the marketplace and the actions taken to date by persons skilled in the art. Stated differently, the Examiner's assessment of the level of ordinary skill in the art under the *Graham Factors* is mistakenly high and is inconsistent with what persons skilled in the art have actually done in the real world.

The article by Samuel K. Moore from the March 2007 issue of *IEEE Spectrum* magazine, entitled "Commercializing quantum keys," submitted in the First office action response, addresses the main issues associated with commercializing quantum cryptography.

The third column, second full paragraph (see highlighted text) of the article makes the important observation that (emphasis added):

"[b]efore customers will accept a new [QKD-based] encryptor, it must pass a certification process ***that can take two or three years***"

This is a direct quote is from SmartQuantum, Inc., a competitor of the Assignee. The passage goes on to say (keeping in mind that encrypted VPNs such as Hoke are certainly known by the declarant), that:

"[W]e do not have the knowledge to develop a fully certified classical encryption system."

This is a clear and definitive statement by a person of ordinary skill in the art that they do not know how to achieve immediate FIPS certification by combining a classically encrypted VPN with their QKD system

The arguments by the Examiner that rely on "a person of ordinary skill in the art" cannot be theoretical arguments that fly in the face of and that are entirely inconsistent with the reality of the documented actions of people skilled in the art in the real world. The Graham Factors require that such information be taken into account.

The second-to-last paragraph of the *IEEE spectrum* article (see highlighted text) states that the system of above-identified Assignee

"...is scheduled for certification by the U.S. National Institute of Standards and Technology in 2007."

This accelerated certification-- as compared to the competition (who by their own admission has not figured out a way to obtain such certification sooner) –is made possible by Assignee's claimed invention.

In short, the Examiner's position set forth in the Second office action on page 7, line 21, that it would have been obvious to combine Hoke and Elliott and the FIPS to achieve a FIPS-compliant QKD system is entirely inconsistent with what is actually happening in the marketplace and as such cannot reasonably be maintained.

Applicant thus respectfully submits that the obviousness rejections of claims 1-16 is traversed and that these claims are patentable over the cited prior art.

CONCLUSION

Applicant respectfully requests that in view of the above remarks, the presently pending claims are in condition for allowance. Accordingly, a Notice of Allowance for the Application is earnestly requested.

Applicant believes that a **one-month** extension of time extension pursuant to 37 C.F.R. § 1.136(a) in the amount of **$60** is necessary to make this Reply timely, and hereby authorizes the Office to charge any necessary fee or surcharge with respect to said time extension to Deposit Account **502992**

Date: **October 14, 2008**

Joseph E. Gortych (Reg. No. 41,791)

Correspondence Address (Customer **#53590**)
Opticus IP Law, PLLC
7791 Alister Mackenzie Dr.
Sarasota, FL 34240

Telephone...941-378-2744
Fax.....321-256-5100
e-mail.....jg@opticus-ip.com